Newsletter Update on the Cybersecurity Framework (July 1, 2015)

Since its release in February 2014, NIST has been educating different sectors about the Framework's use and value. The results of that effort can be seen in the variety of organizations employing the Framework, ranging from multinationals to small businesses. As NIST Director Willie E. May explained to corporate directors and senior executives at a recent National Association of Corporate Directors event, "We see companies like Intel, Chevron, Walgreens, Pepco, Apple, QVC, and the Bank of America talking about how they are using the Framework or planning to incorporate it. But we also see 50-person firms, like Silver Star Communications in rural Wyoming, describing how the Framework has helped them to be more thoughtful and wiser managers of their cyber risks."

Industry Understanding and Use

The proposed value of the Framework has been validated through a large volume and breadth of interactions between NIST and industry. One of the most frequently cited benefits of the Framework is a common cyber risk management language, so that more efficient and precise discussions can be held up, down, and across a company's management structure, with auditors, and with supply chain partners. The Framework is now being used as a basis for security-oriented discussions and decision-making in corporate boardrooms, the C-Suite, and among line managers and staff with cyber responsibilities.

Framework usage and value were further validated at the annual April 2015 RSA conference in San Francisco, where the Framework was perhaps one of the most discussed topics. In his keynote, Federal Communications Commission Chairman, the Honorable Tom Wheeler, highlighted the importance of the Framework in supporting the "New Paradigm" of Business-Driven Cyber Defense. Chairman Wheeler's address also referenced the March release of the FCC Communications, Security, Reliability and Interoperability Council's (CSRIC) Cybersecurity Risk Management and Best Practices Working Group 4: Final Report, which evaluates the merits of the Framework for the telecommunications sector and details recommended adaptation of the Framework to telecommunications subsectors.

Also at the conference, RSA's Michael Brown (retired Rear Admiral) moderated a panel on Using the Cybersecurity Framework, in which Steve Whitlock of Boeing and Tim Casey of Intel outlined their respective companies' use and future plans for the Framework. (Tim also expounded on Intel usage at a separate Intel-specific session.) In that same panel, NIST's Donna Dodson and FCC's David Simpson (retired Rear Admiral) highlighted the continued need for the Framework to be a voluntary tool for making decisions about risk.

In this interview from the conference, Unisys CISO David Frymier highlighted how his company is using the Framework and the value it is bringing.

As revealed in the RSA presentation Risk-Ops at Scale - Framework Operationalization to Address Business Risk, the State of Texas has aligned the Framework Functions to its agency security plan. Texas has developed a statewide

framework that covers cybersecurity best practices and is mapped to the Framework subcategories. To mitigate supplier risk, the state also uses a vendor alignment template that is rooted in the Framework core. Texas has made its Framework resources publically available and we've included a link to it on our Framework Industry Resources webpage.

Continued Outreach

From the onset of Framework development, many companies expressed concern about the growing diversity of cybersecurity requirements around the globe. Because the Framework could standardize vocabulary and organize cybersecurity requirements across multiple nations, NIST continues to reach out to other governments and major multinational corporations. A previous *Status Update* from our team reported that United Kingdom and European Commission representatives have spoken favorably about the Framework and about how our approaches could be aligned with theirs. Since then, NIST has met with officials from more than 20 additional nations, encouraging them to consider the Framework's approach in order to get closer global alignment. Many of those nations are considering the Framework. As recently as May of this year, U.S. Deputy Secretary of Commerce Bruce Andrews led a delegation of 20 American companies on a Cybersecurity Trade Mission to Bucharest, Romania, and Warsaw, Poland. Deputy Secretary Andrews was accompanied by NIST Computer Security Division Chief, Matt Scholl, who addressed a variety of cyber topics including the Framework.

NIST has increased outreach on regulatory alignment in the past six months, particularly in the financial and telecommunications sectors. This included participating in an advisory role to the aforementioned CSRIC Working Group 4. NIST is also an advisory member of the Cybersecurity Forum for Independent and Executive Branch Regulators. The forum was chartered to increase the overall effectiveness and consistency of regulatory authorities' cybersecurity efforts pertaining to U.S. Critical Infrastructure. In all of these interactions, NIST continues to communicate the merits of the Framework as an organizational and communication tool to better manage cybersecurity risk. In the upcoming months, NIST will continue our international and regulatory dialog.

While small and medium businesses (SMB) are well-represented in many of the venues in which we participate, NIST is seeking SMB-specific interactions so we can better understand their needs, challenges, and adoption. Additionally, NIST has begun a campaign to clarify and highlight how the FISMA suite of guidelines and standards (e.g., FIPS-199, SP 800-37rev1, SP 800-53rev4) can be used in concert with the Framework. This effort will bring together federal organizations and other users of FISMA guidance at meetings and other events, and will culminate in a NIST publication.

New and Noteworthy

The latest Industry Resources and Events at the Framework website include:

On 8 April, the NIST Computer Security Division's (CSD) Matt Barrett presented and spent the day at the British Standards Institute (BSI) CIO Summit 2015. Matt

presented on the Framework, and the remainder of the day was spent identifying areas of complement between the ISO27001, the Framework, and related guidance such as the Cloud Security Alliance's (CSA) Cloud Controls Matrix (CCM).

Matt Barrett also presented at the First Clearing Compliance and Risk Management Forum on 10 April in Washington D.C. His presentation encompassed the history, basics, and implementation guidance for the Framework.

In their RSA 2015 presentation "Cookin' Up Metrics with Alex and David," Alex Hutton and David Mortman pronounced the value of the Goal, Question, Metric (GQM) method of creating metrics. Then, they announced a new Society of Information Risk Analysts (SIRA) project for creating Key Risk Indicators and Key Performance Indicators for the Functions, Categories, and Subcategories of the Framework. All are invited to participate in the SIRA NIST CSF Metrics Project.

Also at RSA 2015, Greg Witte and Tom Conkle presented "CForum: A Community Driven Solution to Cybersecurity Challenges." Through the common language established by the Framework, CForum enables collaboration on emerging threats and appropriate measures to combat those threats. All are invited to join the CForum dialog at cyber.securityframework.org.

On 7 May, CSD's Kevin Stine presented "Perspectives on Navigating the Challenges of Cybersecurity in Health Care" via a webinar hosted by AHIP (America's Health Insurance Plans) and Blue Cross/Blue Shield Association (BCBSA).

Adam Sedgewick, NIST Senior IT Policy Advisor, presented at the Spring Consumer Protection Meeting, hosted by the National Association of Attorneys General in Washington D.C. on 11 May.

Donna Dodson, NIST Chief Cybersecurity Advisor, presented at SMi Group's Oil and Gas Cyber Security North America in Houston, Texas on 13 May. Donna's presentation was "Building Resiliency into a Cybersecurity Program."

On 28 May, Adam Sedgewick participated in a U.S. Telecom webinar panel on Telecom Cyber Frameworks, Policies, and Business Processes.

On 1 June, Kevin Stine participated in an AXELOS event to introduce its cyber resiliency best practice guide, Resilia™. Kevin was a member of a panel showing the connections between the AXELOS ITIL service management approach and the Framework.

On June 30, Kevin Stine participated in The Privacy & Security Forum in Chicago, Illinois. Kevin was a panelist on the topic of Navigating a Changing Cyber Landscape – Best Practices and Lessons Learned.

Upcoming

You can learn more about the Framework from NIST speakers at these upcoming public events:

On July 15, Adam Sedgewick is participating in the Atlanta Cybersecurity Roundtable, hosted by the U.S. Chamber of Commerce on Managing Cyber Risks in a Time of State and Non-State Threats to Business Security and Resilience.

Learning & Sharing

NIST's Framework webpage now provides links to Industry Resources at http://nist.gov/cyberframework/cybersecurity-framework-industry-resources.cfm. We believe these initial resources are just a start. If your organization has been using the Framework and has case studies, guidance, tools, mappings, or other information you would like to share more broadly, please contact us at cyberframework@nist.gov. NIST welcomes additions that meet the criteria noted on that page.

The Framework webpage also lists presentations and events – past and future – where NIST is sharing information and experiences about the Framework with current and potential users. Upcoming events can be found at http://nist.gov/cyberframework/cybersecurity-framework-events-presentations.cfm

To assist those who are newer to the Framework, a set of Frequently Asked Questions is now available at: http://nist.gov/cyberframework/cybersecurity-framework-faqs.cfm. If you still have questions after reading the FAQ, send an email to cyberframework@nist.gov.

We are interested in hearing your views on the Framework—positive, negative, and mixed—so we can continue to grow the Framework as a living document, informed by the experiences of those who are using it. Feel free to share or initiate a conversation by sending us a note at cyberframework@nist.gov.